#2

PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: **Tetsuo TAKAGI**

Serial Number: **Not Yet Assigned**

Filed: **January 4, 2001**

For: **FALSIFICATION PREVENTING APPARATUS, FALSIFICATION PREVENTING METHOD AND RECORDING MEDIUM THEREFOR**

CLAIM FOR PRIORITY UNDER 35 U.S.C. 119

Director of Patents and Trademarks
Washington, D.C. 20231

January 4, 2001

Sir:

The benefit of the filing date of the following prior foreign application is hereby requested for the above-identified application, and the priority provided in 35 U.S.C. 119 is hereby claimed:

Japanese Appln. No. 2000-250006, filed on August 21, 2000

In support of this claim, the requisite certified copy of said original foreign application is filed herewith.

It is requested that the file of this application be marked to indicate that the applicant has complied with the requirements of 35 U.S.C. 119 and that the Patent and Trademark Office kindly acknowledge receipt of said certified copy.

In the event that any fees are due in connection with this paper, please charge our Deposit Account No. 01-2340.

Respectfully submitted,
ARMSTRONG, WESTERMAN, HATTORI
McLELAND & NAUGHTON, LLP

Mel R. Quintos
Reg. No. 31,898

Atty. Docket No.: 001738
Suite 1000, 1725 K Street, N.W.
Washington, D.C. 20006
Tel: (202) 659-2930
Fax: (202) 887-0357
MRQ/yap

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

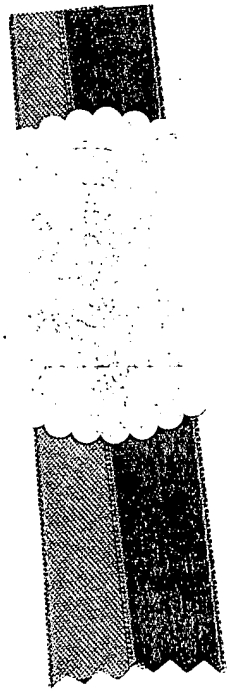
別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　８月２１日

出願番号
Application Number: 特願２０００－２５０００６

出願人
Applicant (s): 株式会社ネットワークドック



CERTIFIED COPY OF
PRIORITY DOCUMENT

２０００年１１月１７日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３０９５０１１

【書類名】　特許願
【整理番号】　P-13965
【特記事項】　特許法第３０条第１項の規定の適用を受けようとする特許出願
【提出日】　平成12年 8月21日
【あて先】　特許庁長官殿
【国際特許分類】　H04L 9/00
【発明の名称】　改ざん防止装置及びその方法
【請求項の数】　5
【発明者】
【住所又は居所】　大阪府大阪市淀川区西中島６丁目１番３号　アストロ新大阪第２ビル　エムオーテックス株式会社内
【氏名】　高木　哲男
【特許出願人】
【識別番号】　500358825
【氏名又は名称】　株式会社ネットワークドック
【代理人】
【識別番号】　100076233
【弁理士】
【氏名又は名称】　伊藤　進
【手数料の表示】
【予納台帳番号】　013387
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　改ざん防止装置及びその方法

【特許請求の範囲】

【請求項１】　インターネット上に公開するページを格納する公開用記録領域と、

前記公開用記録領域に格納されている情報のバックアップ情報を格納するバックアップ記録領域と、

前記公開用記録領域に対する書込み命令を検出する監視手段と、

前記監視手段によって前記公開用記録領域に対する書込み命令が検出されると、前記バックアップ記録領域に格納されているバックアップ情報を前記公開用記録領域にコピーするコピー手段とを具備したことを特徴とする改ざん防止装置。

【請求項２】　前記公開用記録領域に格納されている情報を更新するための更新用記録領域を更に有し、

前記コピー手段は、前記更新用記録領域に格納されている情報が更新されると、前記更新用記録領域に格納されている情報を前記公開用記録領域及び前記バックアップ記録領域にコピーすることを特徴とする請求項１に記載の改ざん防止装置。

【請求項３】　前記更新用記録領域の更新時にユーザー認証を実行する認証手段を更に具備したことを特徴とする請求項２に記載の改ざん防止装置。

【請求項４】　インターネット上に公開するページを格納する公開用記録領域に対する書込み命令を検出する手順と、

前記公開用記録領域に対する書込み命令を検出すると、前記公開用記録領域に格納されている情報のバックアップ情報を格納するバックアップ記録領域から前記バックアップ情報を読出して前記公開用記録領域にコピーする手順とを具備したことを特徴とする改ざん防止方法。

【請求項５】　ユーザー認証が実行されると、前記公開用記録領域及び前記バックアップ記録領域の情報を更新可能にする手順を更に具備したことを特徴とする請求項４に記載の改ざん防止方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、インターネット上のＷｅｂサーバに好適な改ざん防止装置及びその方法に関する。

【０００２】

【従来の技術】

近年、インターネットが急速に普及してきている。特に、Ｗｅｂサーバへのアクセス（Ｗｅｂアクセス）は、インターネット上における各種情報の公開及び取得を容易にしており、広く普及している。インターネットのWWW（World Wide web）上における情報の公開先を通常「ホームページ」と呼び、このホームページをＷｅｂサーバ上に格納することによって、情報の公開が行われる。

【０００３】

ユーザーは、インターネット上に接続されたパソコン上のＷｅｂブラウザソフトを利用して、ホームページのアドレスであるＵＲＬを指定することで、Ｗｅｂサーバにアクセスして所望の情報（ページ）をダウンロードして表示させることができる。

【０００４】

しかしながら、近年、Ｗｅｂサーバ上のホームページに不正アクセスし、改ざん等を行うハッカー，クラッーカー等が増加してきた。これらの不正侵入者は、例えば、Ｗｅｂサーバのセキュリティホールを利用してＷｅｂサーバに不正に侵入し、ホームページ内の情報を改ざんする。

【０００５】

このような不正侵入者の不正アクセスを未然に防ぐために、情報公開者側がファイアウォールを構築することが考えられる。しかしながら、セキュリティレベルを高く設定するためには、ファイアウォールを高度に構築する必要があり、また、セキュリティ管理も煩雑である。しかも、一端ファイアウォールを越えて不正侵入されると、Ｗｅｂサーバの改ざん等を阻止することができない。

【０００６】

そこで、ファイルが改ざんされたことを、チェックサムの計算等によって検出

して、管理者に通知するシステムが考えられている。この手法では、ファイル全体の特徴を抽出して小さなビット列に変換した値をチェックサムとして用いている。元のファイルのチェックサムの値を監視することで不正な改ざんを検知するのである。

【０００７】

【発明が解決しようとする課題】

しかしながら、ファイルのチェックサムを監視して不正な改ざんを検知する手法では、監視のための演算及びチェックサムの記録のために極めて大きなＣＰＵ能力及び記録容量を必要とするという問題点があった。

【０００８】

本発明はかかる問題点に鑑みてなされたものであって、大きなＣＰＵ能力及び記録容量を必要とすることなく、改ざん直後に元のファイルに自動的に戻すことを可能にすることにより改ざんを防止することができる改ざん防止装置及びその方法を提供することを目的とする。

【０００９】

【課題を解決するための手段】

本発明の請求項１に係る改ざん防止装置は、インターネット上に公開するページを格納する公開用記録領域と、前記公開用記録領域に格納されている情報のバックアップ情報を格納するバックアップ記録領域と、前記公開用記録領域に対する書込み命令を検出する監視手段と、前記監視手段によって前記公開用記録領域に対する書込み命令が検出されると、前記バックアップ記録領域に格納されているバックアップ情報を前記公開用記録領域にコピーするコピー手段とを具備したものであり、

本発明の請求項４に係る改ざん防止方法は、インターネット上に公開するページを格納する公開用記録領域に対する書込み命令を検出する手順と、前記公開用記録領域に対する書込み命令を検出すると、前記公開用記録領域に格納されている情報のバックアップ情報を格納するバックアップ記録領域から前記バックアップ情報を読出して前記公開用記録領域にコピーする手順とを具備したものである。

【００１０】

本発明の請求項１においては、インターネット上に公開するページを格納する公開用記録領域とバックアップ情報を格納するバックアップ記録領域とを有する。公開用記録領域に対して書込み命令が発生すると、監視手段はこの書込み命令を検出する。コピー手段は、監視手段によって書込み命令が検出されると、バックアップ記録領域に格納されているバックアップ情報を公開用記録領域にコピーし、改ざんされた公開用記録領域を自動的に修復する。

【００１１】

本発明の請求項４において、公開用記録領域に対する書込み命令が発生するとこの書込み命令が検出される。公開用記録領域の内容を検査することなく公開用記録領域の改ざんが検出される。公開用記録領域に対する書込み命令が検出されると、バックアップ記録領域に格納されているバックアップ情報を公開用記録領域にコピーする。これにより、改ざんされた公開用記録領域が自動的に修復される。

【００１２】

【発明の実施の形態】

以下、図面を参照して本発明の実施の形態について詳細に説明する。図１は本発明に係る改ざん防止装置の一実施の形態を示すブロック図である。また、図２は改ざん防止システムを説明するための説明図である。

【００１３】

図２において、インターネット１１上には複数のパソコン１２及び各種インターネット端末１３が接続されている。情報公開者のネットワーク１４は、ルータ１５を介してインターネット１１に接続されている。ルータ１５とＷｅｂサーバ１７との間にはファイアーウォール１６が設けられており、ファイアーウォール１６は、インターネット１１上からのＷｅｂサーバ１７への不正アクセスを防止することができるようになっている。

【００１４】

例えば、ファイアーウォール１６は、ＨＴＴＰプロトコロ等のリクエストについてはＷｅｂサーバ１７に与え、そのレスポンスをインターネット１１上に送出

する。しかし、ファイアーウォール１６は、その他の許可しないプロトコル、サーバ及び端末等のアクセスを禁止することができるようになっている。ファイアーウォール１６は、アプリケーション毎のアクセス制限を可能にする。

【００１５】

Ｗｅｂサーバ１７は、例えば、ＯＳ（オペレーションシステム）としてＷｉｎｄｏｗｓ　ＮＴ（登録商標）を採用し、Ｗｅｂアクセスに応答した処理を実行することができるようになっている。即ち、Ｗｅｂサーバ１７は、ＨＴＴＰプロトコル等のリクエストに応答して、指定されたファイルをレスポンスとして送出する。

【００１６】

本実施の形態においては、Ｗｅｂサーバ１７は、公開用ディレクトリ１８にホームページを格納すると共に、この公開用ディレクトリ１８のバックアップ用の複数のバックアップディレクトリ１９，１９，…を有している。Ｗｅｂサーバ１７は、所定時間毎に、公開用ディレクトリ１８とバックアップディレクトリ１９，１９…との同期をとっており、公開用ディレクトリ１８が改ざんされると、自動的にバックアップディレクトリ１９の内容によって公開用ディレクトリ１８を更新することができるようになっている。

【００１７】

また、Ｗｅｂサーバ１７は、Ｗｅｂページ更新用ディレクトリ２１を有しており、Ｗｅｂページ更新用ディレクトリ２１の内容で公開用ディレクトリ１８及びバックアップディレクトリ１９を更新することができるようになっている。ホームページの本来の書換え時には、Ｗｅｂページ更新用ディレクトリ２１を書き換えることで、ホームページを更新して公開することが可能である。

【００１８】

図１は図２のＷｅｂサーバ１７を構成するコンピュータ上に組込まれる改ざん防止装置の具体的な構成を示すブロック図である。

【００１９】

Ｉ／Ｏ（入出力部）８は図２のファイアーウォール１６に接続される。入力装置７は、キーボード等によって構成され、ユーザー操作に基づく信号を制御部１

に出力して、制御部１に対して各種の指示を行う。

【００２０】

制御部１は、Ｗｉｎｄｏｗｓ　ＮＴ等のＯＳや、サーバソフト等によって実現されるものであり、入力装置７からの信号に基づいて動作して、各部を制御するようになっている。

【００２１】

記録部２は、ハードディスク等によって構成されており、図２の公開用ディレクトリ、バックアップディレクトリ及びＷｅｂページ更新用ディレクトリ等を格納する領域を有する。書込み読出し制御部３は、記録部２の書込み及び読出しを制御する。記録部２は、書込み読出し制御部３に制御されて、制御部１からの情報を記録すると共に、記録した情報を読出して制御部１に与えるようになっている。

【００２２】

制御部１は、Ｉ／Ｏ８からホームページのリクエストが入力されると、書込み読出し制御部３を制御して、記録部２の公開用ディレクトリに記録されているホームページを読出し、Ｉ／Ｏ８を介してレスポンスとしてインターネット１１に送出するようになっている。

【００２３】

本実施の形態においては、書込み読出し制御部３が公開用ディレクトリに対して書込み指示を与えたか否かを検出する監視部４が設けられている。監視部４は、公開用ディレクトリに対して書込みが発生したことを検出して改ざん検出信号を制御部１に出力するようになっている。また、本実施の形態においては、バックアップディレクトリの内容を公開用ディレクトリにコピーするためのコピー制御部６も設けられている。コピー制御部６は、制御部１に制御されて、書込み読出し制御部３に指示を与えてデータのコピーを行うようになっている。

【００２４】

制御部１は、監視部４から改ざん検出信号が入力されると、コピー制御部６を制御して、バックアップディレクトリの内容を公開用ディレクトリにコピーさせるようになっている。また、コピー制御部６は、Ｗｅｂページ更新用ディレクト

リに対して更新が行われると、制御部１に制御されて、Ｗｅｂページ更新用ディレクトリの内容をバックアップディレクトリ及び公開用ディレクトリにコピーするようになっている。

【００２５】

なお、コピー制御部６によるコピー動作時には、監視部４の監視は無効にされるようになっている。

【００２６】

また、制御部１は、改ざん検出信号が入力されると、Ｉ／Ｏ８を介してネットワーク１４上の図示しない管理者用コンピュータに対して、改ざんが発生したことを通知すると共に、図示しない表示部に対して改ざんが発生したことを示す表示を表示させることができるようになっている。

【００２７】

認証部５は、書込み読出し制御部３によって、記録部２のＷｅｂページ更新用ディレクトリ及びバックアップディレクトリに対する書込み時には、ユーザー認証を要求するようになっている。制御部１は、認証部５によってユーザー認証が要求されると、ユーザー認証が要求されていることを表示部等によって表示させ、例えば、Ｉ／Ｏ８を介して又は入力装置７等によって、ユーザーＩＤ及びパスワード等をユーザーに入力させるようになっている。認証部５は、ユーザー認証が行われた場合にのみ、記録部２への書込みを許可するようになっている。

【００２８】

次に、このように構成された実施の形態の動作について説明する。

【００２９】

いま、インターネット１１上のパソコン１２を利用可能なユーザーが、公開されたＷｅｂサーバにアクセスして、ホームページの情報を取得するものとする。ユーザーはパソコン１２上において、ブラウザソフトを起動して、ホームページのＵＲＬを入力する。パソコン１２からのリクエストは、インターネット１１を介して情報公開者のネットワーク１４に伝送される。ルータ１５はインターネット１１を介して伝送されたリクエストを、ファイアーウォール１６を介してＷｅｂサーバ１７に供給する。このリクエストは、Ｉ／Ｏ８を介して制御部１に伝送

される。

【００３０】

制御部１は、リクエストに応じて書込み読出し制御部３を制御し、記録部２の公開用ディレクトリに格納されているホームページの情報を読出して、Ｉ／Ｏ８からレスポンスとして送出する。このレスポンスは、ファイアーウォール１６及びルータ１５を介してインターネット１１上に送出され、パソコン１２に取込まれる。こうして、パソコン１２上で起動されているブラウザソフトは、受信したレスポンスに基づいて、ホームページを表示する。こうして、インターネット１１上のユーザーは、ブラウザソフト上で、情報公開者が提供するホームページを見ることができる。

【００３１】

ここで、インターネット１１上のユーザーが何らかの手段によってファイアーウォール１６内に不正に侵入して、Ｗｅｂサーバ１７内のホームページを改ざんするものとする。不正侵入者による書込み命令は、制御部１によって書込み読出し制御部３に供給される。読出し制御部３は、記録部２の公開用ディレクトリに対して書込みを行う。

【００３２】

一方、監視部４は、書込み読出し制御部３による書込み命令を検出しており、改ざん検出信号を制御部１に出力する。そうすると、制御部１は、コピー制御部６に対して、バックアップディレクトリの内容を公開用ディレクトリにコピーさせる。監視部４が比較的短い周期で改ざんを監視することにより、極めて短時間にバックアップディレクトリによる復旧が可能である。例えば、コピー制御部６は、改ざんが開始された後の数ミリ秒程度で、バックアップディレクトリの内容のコピーを開始することができる。

【００３３】

従って、この場合には、不正侵入者による改ざんが行われると略同時に元のデータへの復旧が行われることになり、他の一般ユーザのパソコン上には、改ざんが行われていない状態のホームページが表示される。なお、不正侵入者による改ざんの検出から、所定時間後に、データを元のデータに復旧させるようにしても

よい。

【００３４】

監視部４は、公開用ディレクトリに対する書込み命令を検出することで改ざんの有無を監視しており、公開用ディレクトリの解析等は行っておらず、改ざん検出のために大容量の記録部は不要であり、また、高いＣＰＵ能力も不要である。

【００３５】

監視部４は、例えばＷｉｎｄｏｗｓ　ＮＴの機能を用いて実現することができ、制御部１は、改ざん検出信号によって割り込み命令を発生して、コピー制御を行うことで、改ざんの監視及びデータの復旧を容易に且つ迅速に行うことができる。

【００３６】

次に、情報公開者自らが公開用ディレクトリを更新するものとする。この場合には、情報公開者は、例えば入力装置７によって公開用ディレクトリの更新を指示する。制御部１は、更新指示を書込み読出し制御部３に出力して、Ｗｅｂページ更新用ディレクトリの書込みを行う。この書込みに際して、認証部５は、ユーザー認証を要求する。制御部１は、ユーザー認証のための表示を表示部に表示させる。ユーザーは、ユーザー認証のためのＩＤ及びパスワード等を入力装置７によって入力する。認証部５は、ユーザの入力操作によるＩＤ及びパスワードが予め登録されている情報と一致している場合にのみ、Ｗｅｂページ更新用ディレクトリの書込みを許可する。これにより、不正侵入者によるＷｅｂページ更新用ディレクトリの書込みは阻止される。なお、不正侵入者によるバックアップディレクトリに対する書込みも阻止されることは同様である。

【００３７】

ユーザー認証が行われると、書込み読出し制御部３は、Ｗｅｂページ更新用ディレクトリをユーザ操作に基づいて更新する。コピー制御部６は、Ｗｅｂページ更新用ディレクトリ、バックアップディレクトリ及び公開用ディレクトリの同期をとっており、Ｗｅｂページ更新用ディレクトリが更新されると、Ｗｅｂページ更新用ディレクトリの内容をバックアップディレクトリ及び公開用ディレクトリにコピーする。こうして、公開用ディレクトリの更新が行われる。

【００３８】

このように、本実施の形態においては、公開用ディレクトリに対する書込みを検出することで改ざんを検出しており、改ざんの検出から短時間でバックアップディレクトリの内容を公開用ディレクトリにコピーして公開用ディレクトリを改ざんから自動修復させるようになっている。これにより、大容量の記録部及び高い能力のＣＰＵを必要とすることなく、改ざんを防止することができる。

【００３９】

なお、情報公開者による公開用ディレクトリの更新時には、改ざんの検出及びコピーによる自動修復機能を一時停止させるようにしてもよい。この場合には、直接公開用ディレクトリ又はバックアップディレクトリ等を更新することができる。

【００４０】

なお、記録部２は１つのハードディスクで構成するのではなく、複数のハードディスク或いは複数種類の記録メディアによって構成することができる。また、例えば、電気通信回線によって、他の記録メディアに記録された公開用ディレクトリ、バックアップディレクトリ及びＷｅｂページ更新用ディレクトリ間で同期をとりコピーを行うようにしてもよいことは明らかである。

【００４１】

【発明の効果】

以上説明したように本発明によれば、大きなＣＰＵ能力及び記録容量を必要とすることなく、改ざん直後に元のファイルに自動的に戻すことを可能にすることにより改ざんを防止することができるという効果を有する。

【図面の簡単な説明】

【図１】

本発明に係る改ざん防止装置の一実施の形態を示すブロック図。

【図２】

改ざん防止システムを説明するための説明図。

【符号の説明】

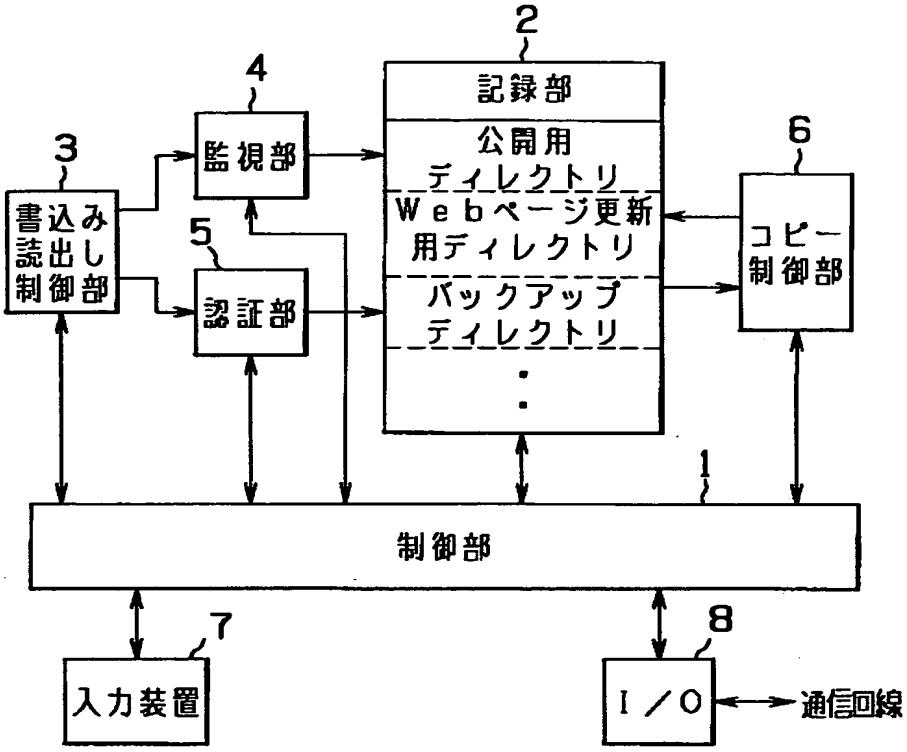
１…制御部、２…記録部、３…書込み読出し制御部、４…監視部、５…認証

部、６…コピー制御部、７…入力装置、８…Ｉ／Ｏ。

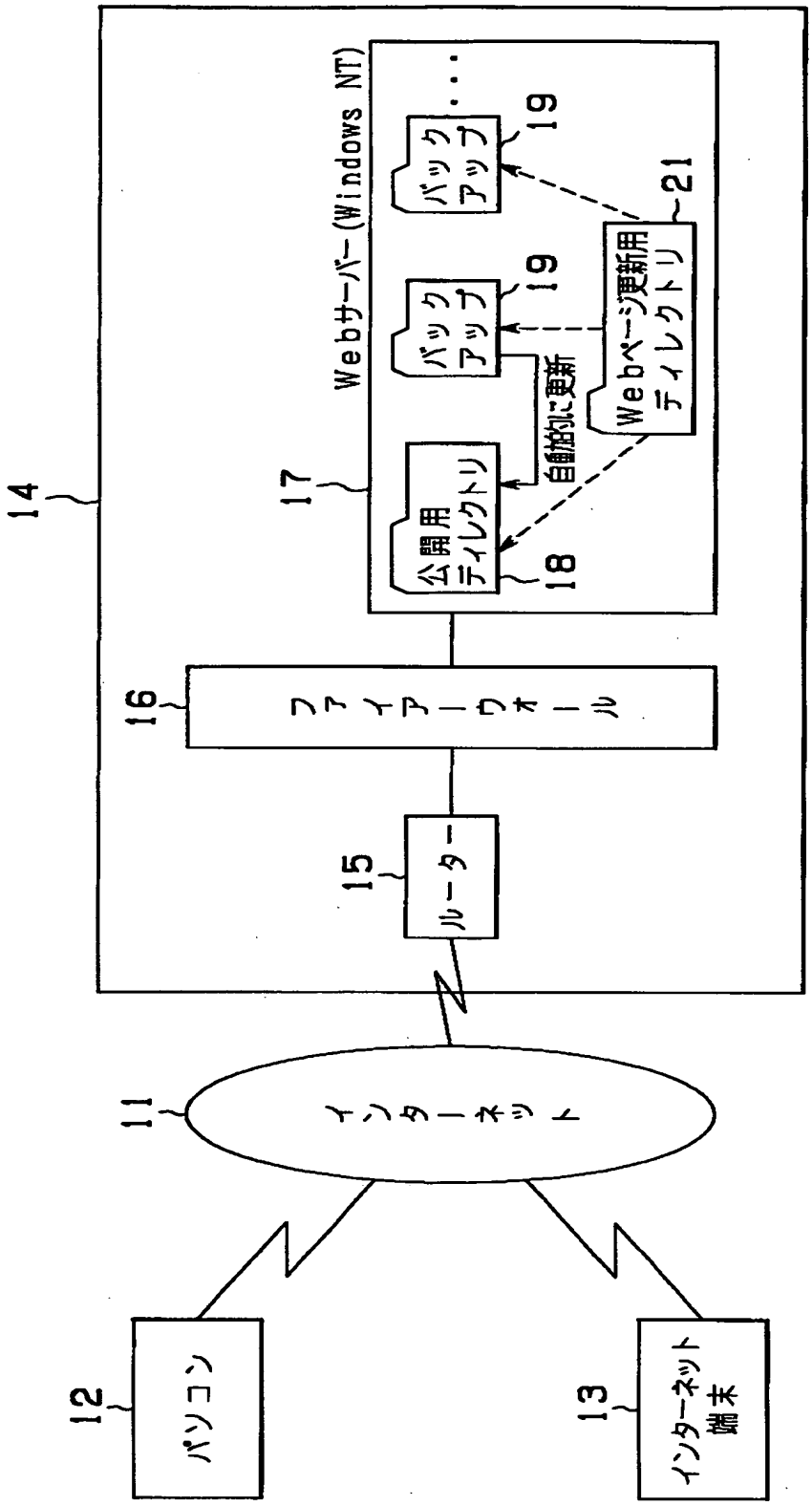
代理人　　弁理士　　伊　藤　　進

【書類名】　　図面

【図１】


2
記録部
公開用
ディレクトリ
Webページ更新
用ディレクトリ
バックアップ
ディレクトリ
4
監視部
3
書込み
読出し
制御部
5
認証部
6
コピー
制御部
1
制御部
7
入力装置
8
I／O
通信回線

【図２】


14
Webサーバー(Windows NT)
17
公開用ディレクトリ
18
バックアップ
19
バックアップ
19
バックアップ
19
自動的に更新
Webページ更新用ディレクトリ
21
16
ファイアーウォール
15
ルーター
11
インターネット
12
パソコン
13
インターネット端末

【書類名】　　要約書

【要約】

【課題】Ｗｅｂページの改ざんを防止する。

【解決手段】監視部４は、書込み読出し制御部３による記録部２の公開用ディレクトリに対する書込み命令を検出する。制御部１は、監視部４から改ざん検出信号が入力されると、コピー制御部６を制御して、バックアップディレクトリに格納されている情報を読出して公開用ディレクトリにコピーする。これにより、公開用ディレクトリの改ざんが防止される。書込み命令の検出によって改ざんを検出しており、改ざんの検出に大容量の記録装置及び高いＣＰＵ能力を必要としない。

【選択図】　　図１

出 願 人 履 歴 情 報

識別番号　　〔５００３５８８２５〕

１．変更年月日　　２０００年　７月２５日
［変更理由］　新規登録
住　所　東京都中央区日本橋浜町３丁目１９番２号
氏　名　株式会社ネットワークドック